IN THE DISTRICT COURT OF THE UNITED STATES
FOR THE DISTRICT OF SOUTH CAROLINA
SPARTANBURG DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. APPROXIMATELY 199,990 USDT, Defendant *in Rem*.	)	CIVIL ACTION NO.: 7:24-cv-05458-JDA

UNITED STATES' COMPLAINT FOR FORFEITURE *IN REM*

The Plaintiff, United States of America, brings this complaint and alleges as follows, in accordance with Rule G(2) of the Supplemental Rules for Admiralty and Maritime Claims and Asset Forfeiture Actions.

NATURE OF THE ACTION

1. This is a civil action *in rem* to forfeit to the United States of America funds in the amount of Approximately 199,990 USDT valued at approximately $199,990 USD ("United States Dollars"), ("Defendant Funds"), pursuant to 18 U.S.C. § 981(a)(1)(A) and 18 U.S.C. § 981(a)(1)(C). The United States seeks forfeiture based upon a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitute, or are traceable to:

a. property involved in wire fraud transactions, attempted wire fraud transactions, or conspiracy of same in violation of 18 U.S.C. §§ 1343, 1349;

b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i), and/or § 1956(a)(1)(B)(i) and/or 1957;

c. property involved in an illegal money transmitting business, in violation of 18 U.S.C. § 1960; and/or

d. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(c)(7) and;

e. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(h) and;

f. property involved in money transactions in criminally derived property or attempted money transactions, in violation of 18 U.S.C. § 1957.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction over an action commenced by the United States pursuant to 28 U.S.C. § 1345, and over an action for forfeiture by virtue of 28 U.S.C. § 1355. This Court has *in rem* jurisdiction over the Defendant Funds pursuant to:

(a) 28 U.S.C. § 1355(b)(1)(A), because acts or omissions giving rise to the forfeiture occurred in the District of South Carolina; and

(b) 28 U.S.C. § 1355(b)(1)(B), because venue properly lies in this district pursuant to 28 U.S.C. § 1395.

THE DEFENDANT *IN REM*

3. The Defendant Funds consist of approximately 199,990 USDT valued at approximately $199,990.00 USD, obtained by agents with the United States Secret Service ("USSS") during an investigation into a transnational criminal organization running an exploitation of elderly and social engineering scam. The funds were seized from a cryptocurrency custodial wallet under the

control of Binance, identified by account number 535878518 (the "Subject Account"), and under the name of Cristina Paola ("PAOLA"). PAOLA is a resident of Maracaibo, Venezuela.

4. The USSS seized the approximately 199,990 USDT valued at approximately $199,990.00 USD, for federal forfeiture. The Defendant Funds are currently restrained and pending deposit to an account under the control of United States Secret Service.

5. In accordance with the provisions of 19 U.S.C. § 1606, the Defendant Funds have a total domestic value of approximately $199,990.00.

KNOWN POTENTIAL CLAIMANTS

6. The known individuals whose interests may be affected by this litigation are:

a. Cristina Paola, who may have an interest in the Defendant Funds because she was the named account holder of the account seized by USSS during this investigation.

BASIS FOR FORFEITURE

7. Pursuant to the pleading requirements of Supplemental Rule G(2)(f), Plaintiff alleges that there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds are subject to forfeiture to the United States, based in part upon the following:

a. USSS and local law enforcement agencies were investigating a transnational criminal organization running an exploitation of elderly and social engineering scam. In brief summary, investigating agents determined that a scamming group has been using social engineering to contact elderly individuals and convince them that their bank accounts are compromised. Once the scammers have engagement from the victim, they

instruct them that their bank accounts are compromised and that they need to put their funds in a secure location while they investigate. The victims then withdraw their funds in cash and take it to a BTC Automated Teller Machine ("ATM"). From that ATM, the funds are sent to a cryptocurrency wallet address provided by the suspects.

b. Digital currency (also known as virtual currency or cryptocurrency)[1] is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency[1] or other cryptocurrencies. Examples of cryptocurrency are Bitcoin (BTC), Litecoin (LTC), Ethereum (ETH) and Tether (USDT). Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud- based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[2] Cryptocurrency is not illegal in the United States.

[1] For purposes of this complaint, the terms "digital currency," "cryptocurrency," and "virtual currency" are used interchangeably and address the same concept.

c. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

d. Although cryptocurrencies such as Bitcoin, Ethereum and Tether have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is often used as payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track transactions.

e. BTC Value in U.S. Dollars: As of March 7, 2024, one BTC is worth approximately $67,944, though the value of BTC is generally much more volatile than that of fiat currencies.

f. Cryptocurrency "exchangers" and "exchanges" are individuals or companies that exchange bitcoin for other currencies and cryptocurrencies, including U.S. dollars and Tether/USDT. Exchanges can be brick-and-mortar businesses or online businesses (exchanging electronically transferred money and virtual currencies). According to Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.[3] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). Based on my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit

exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%).

g. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code[4] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency

wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

h. Binance is a global cryptocurrency spot and derivatives exchange. Binance serves customers from around the world. There is no official company headquarters, but the organization was founded in 2017 in Shanghai, China.

i. What is common across many exploitations of the elderly and elder abuse cases when it comes to cryptocurrency, is that they initially contact the victim from a point of perceived authority to the victim. They do this through email, text message, and sometimes computer access through a point of compromise such as a virus or clicking a fraudulent link. This can be as sophisticated as impersonating law enforcement or purporting to be from their bank's corporate security. Once the suspect engages with the victims, they often request that they hide or lie about their actions as to not raise suspicion from actual authorities. From this point, they convince the victim to withdraw their own funds from their accounts and forward it to the suspect through various means. A common method it is to have the victim deposit cash into a Bitcoin ATM and send the transaction to a wallet address provided to the victim.

j. On or about December 18, 2023, S.L. and her disabled husband, residents of Campobello, S.C. lost access to their crypto currency account at Coinbase. They were contacted by an individual who portrayed themselves to be tech support with Coinbase,

and inadvertently provided them with access to their account. A few hours later, they were able to regain access to their account and found that approximately $350,000.00 of Ethereum (ETH) had been transferred out to wallet address, 0x7d695F5652218F978A09c7b532e469Eb34DcD0F0.

k. Law enforcement reviewed the transaction history for the digital currency wallet 0x7d695F5652218F978A09c7b532e469Eb34DcD0F0 ("Wallet 1") in a commercial blockchain analysis platform. On December 18, 2023, at 18:09 Hrs UTC 151.39543308 ETH was deposited into the wallet address via transaction ID: 0x7616de9ce99f15bc348494e4c6a64b4da1838bde240fc6f81ae618d029418966. This deposit was likely from the account of S.L. and matches the transaction shown from the Coinbase account. Further, this wallet address remained dormant without any activity for over two years. The previous activity dating back to 2021 included simply pass through transactions in which cryptocurrency would be deposited in and immediately transferred out, serving no true investment or business purpose.

l. The victim's cryptocurrency passed through intermediary wallet addresses or "Burn Wallets ," was converted from Ethereum (ETH) to Tether (USDT), and transferred on. At one point, the USDT remained in a cold wallet without activity for almost two months prior to rapidly moving between several wallets before landing and being held in the Binance account 535878518 (Subject Account) in the customer name of Cristina Paola ("PAOLA").

m. In detail, after funds were deposited from the victim's Coinbase account into wallet

address 0x7d695F5652218F978A09c7b532e469Eb34DcD0F0 (Wallet 1), they remained in that wallet for only eight minutes prior to being sent out to wallet address 0x7EB4Af512b24C858A0571963e6e8a6051C56317F (Wallet 2) via transaction hash: 0x210f2eeae61cc302f9159ef52b4201079745e8bb7fe2ac322502b5be0acfb353.

n. The funds were then sent out from that wallet address approximately thirty minutes later in four transactions being sent to Changenow.io. This is a non-custodial service that converts cryptocurrencies to other types of cryptocurrencies, and forwards on to the wallet and network specified. The funds were converted from ETH to USDT and forwarded onto wallet address TMwmkAqDFwwNctdy5R6JpiAWtZUGuCRzmK (Wallet 3), via five divided up transactions. This address is hosted on the TRON Network and appears to only be a burn wallet which was created and had activity in it for only six days. All of the activity in this account, which exceeded half a million dollars in six days, was simply deposits and immediate withdraws, indicating that this wallet was only used to further obscure and hide the illicit activity.

o. Immediately after the final deposit from CHangenow.io, approximately eight minutes later, the funds were withdrawn in a single transaction of 475,952.318313 USDT to wallet address TJKaqv2dPq3m7Wi9BLxpSXqPG3AMd3iwNn (Wallet 4), via transaction hash: ae62814d7fb9020161416e08cb14af70b661cc507707315498f3d9cd81b241a7. The very next transaction out of that wallet was a transaction of 494,000.00 USDT to wallet

address TE6EdovBHsRha7Qy1WUgsBGqL3HFjWHyaz (Wallet 5) via transaction hash: 973f6a85b55c21612bb3252fc55c8a26455ac9e1396453233bab2923acd09463.

p. After the receipt of that transaction, Wallet 5 sent out the USDT in several transactions, two of which sent a total of 202,000 USDT to wallet address TDovHpPDAYpKtyCT5s2hnnGJL2FvajA9yT (Wallet 6) via transaction hashes: 3e830e744a98b855e53a836b63710016ca2ca62f618a66395abcf78f840c9b54 and d908835717733cfa0de62e755598944db71cfe9a40faef55d2d053c8b50c1b4b. All of these transactions occurred within the first 24hrs of the initial theft from the victim's account. Once the funds were deposited into Wallet 6, they remained dormant with no account activity for approximately a month and a half. This is often done to further try and obscure the activity and throw off investigative activity.

q. On February 6th, 2024, at 1408 Hrs a test transaction of 100 USDT was sent out of Wallet 6 and sent to wallet address TGjbuaKMPwoscPy9BnMw7TJkJ41cNkoJ6W (Wallet 7) via transaction hash: 4d087c0fddcd3e851d973f5657f00a9cb1f266697b5d5caf911135d3ba94cdaf. Test transactions are often done to verify whether or not the account has been locked down by investigators or to ensure the funds are sent to the correct person. Once confirmed that the wallet address has not been not locked down, the remainder of the victim's funds were sent to Wallet 7.

r. Once the entirety of the funds were received by Wallet 7, they were sent out in a single transaction of 202,000.00 USDT to wallet address

TPuKFDcecgo5XoWU7N5VnAyQxXFihKBGpy (Wallet 8) via transaction hash: c20ce5b6140ca76b350def6d2ffdaa8461508825068bcdd5b0cdf9d61a1b7052. After less than a minute of receiving the funds, Wallet 8 sent the funds back out to wallet TWmzne9aBiARP77YgLACsxWzUkjHYrsSrq (Wallet 9) via transaction hash: 022dd8c6399121a2a0cba5823f7d5f312bcab822024e9e508f01f33a3b7ce9bb. This extremely rapid movement was done to further attempt to obscure the illicit activity.

s. Immediately after receiving the funds into Wallet 9, 200,000 USDT of the victim funds were sent out four minutes later to wallet address TNfJQ77qvAgLwtEcEkwiwcyAPD5BdppugB (Wallet 10), via transaction hash: 0cdeedab1498d5c47793c2ec0f091b8965e0fdf5c9413a5ae9fbcacd0bd693a1. Once funds were received into Wallet 10, three hours later, a 100 USDT test transaction was sent to wallet address TJckw8jfx3jPrqfuF8dfBAZ2Qt9Aeadxfq (Suspect Wallet), which is hosted at Binance and in the customer name of PAOLA. A few hours later after the transaction was confirmed, the remaining -199,900.00 USDT of the victim's funds was transferred to the same Suspect Wallet via transaction hash: 2cac816eadfd626fad700d0a5d965093c376909d355e36fe2cc899dff8c0eaa1. It was at this point, when the funds were transferred to Binance, that Binance investigations placed a voluntary hold on the Subject Account.

t. Binance identified PAOLA as the account holder of Suspect Wallet. Between January, 2023 and February 7, 2024, this Suspect Wallet received 204 deposits totaling approximately $6,607,441.81 and sent 130 transactions totaling approximately

$3,828,062.20. The activity in the account in relation to the deposits and withdraws consists of almost exclusively receiving funds and quickly sending them back out. The wallet addresses in which these funds were received and sent to are also the same pairing of wallet addresses, indicative of a money laundering operation. The volume of transactions in the Subject Account is highly suspicious, as more than $5 million USD equivalent of digital currency moved through the wallet associated with the Subject Account in less than 1 year. The Subject Account did not appear to hold digital currency for long, instead rapidly receiving and then retransmitting digital currency, and often in the form of stablecoins. The Subject Account did not appear to be engaged in any investment activity, as digital currency rapidly moved in and out, and stablecoins are designed not to increase in value greater than the USD. While these amounts might be unsurprising in a commercial or business account, the Subject Account was opened as a personal account with no identified associated business. Public information searches for PAOLA do not identify any legitimate businesses associated with PAOLA which would justify a personal account receiving and sending these volumes of digital currency.

u. A federal seizure warrant was obtained and executed for the Target Cryptocurrency Wallet, under the control of Binance. Binance remitted the approximately 199,990.00 USDT on July 19, 2024, pursuant to the seizure warrant.

8. Based on the information and allegations set forth herein, there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitutes, or is traceable to:

a. property involved in wire fraud transactions, attempted wire fraud transactions, or conspiracy of same in violation of 18 U.S.C. §§ 1343, 1349;

b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i), and/or § 1956(a)(1)(B)(i) and/or 1957;

c. property involved in an illegal money transmitting business, in violation of 18 U.S.C. § 1960; and/or

d. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(c)(7);

e. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(h) and;

f. property involved in money transactions in criminally derived property, in violation of 18 U.S.C. § 1957.

CONCLUSION

9. By reason of these premises, and pursuant to 18 U.S.C. § 981(f) and 21 U.S.C. § 881(h), whereby the Plaintiff's right, title and interest in and to the Defendant Funds relates back to the commission of the act giving rise to the forfeiture, the Defendant Funds has become and is forfeited to the United States of America, to be disposed of pursuant to Supplemental Rule G(7)(c) for Admiralty or Maritime Claims and Asset Forfeiture Actions, 18 U.S.C. § 981(d), 21 U.S.C. § 881(e), and other applicable laws.

WHEREFORE, Plaintiff prays that due process issue to enforce the forfeiture of the Defendant Funds, *in rem*; that a Warrant for the Arrest of the Defendant Funds be issued; that due

Notice be given to all interested persons to appear, make claim, answer and show cause why the forfeiture should not be decreed; that the Defendant Funds be decreed condemned and forfeited to the United States of America for disposition according to law; and that Plaintiff have such other and further relief as the Court may deem just and proper, together with the costs and disbursements of this action.

Respectfully submitted,

ADAIR F. BOROUGHS
UNITED STATES ATTORNEY

By: *s/Carrie Fisher Sherard*
Carrie Fisher Sherard #10134
Assistant United States Attorney
55 Beattie Place, Suite 700
Greenville, SC 29601
(864) 282-2100

October 1, 2024